

ANTIVIRUS SOFTWARE

1949–1980 period (pre-antivirus days)	4
1980–1990 period (early days)	5
1990–2000 period (emergence of the antivirus industry)	6
2000–2005 period	7
2005 to present	8
Signature-based detection	10
Heuristics	11
Rootkit detection	11
Real-time protection	11
Unexpected renewal costs	12
Rogue security applications	12
Problems caused by false positives	12
System and interoperability related issues	13
New viruses	15
Rootkits	15
Damaged files	15
Firmware issues	16

Antivirus software



Antivirus or anti-virus software (often abbreviated as AV), sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect from: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DDoS attacks.

History

1949–1980 period (pre-antivirus days)

Although the roots of the computer virus date back as early as 1949, when the Hungarian scientist John von Neumann published the *"Theory of self-reproducing automata"*, the first known computer virus appeared in 1971 and was dubbed the "Creeper virus". This computer virus infected Digital Equipment Corporation's (DEC) PDP-10 mainframe computers running the TENEX operating system.

The Creeper virus was eventually deleted by a program created by Ray Tomlinson and known as "The Reaper". Some people consider "The Reaper" the first antivirus software ever written – it may be the case, but it is important to note that the Reaper was actually a virus itself specifically designed to remove the Creeper virus.

The Creeper virus was followed by several other viruses. The first known that appeared "in the wild" was "Elk Cloner", in 1981, which infected Apple II computers.

In 1983, the term *"computer virus"* was coined by Fred Cohen in one of the first ever published academic papers on computer viruses. Cohen used the term *"computer virus"* to describe a program that: *"affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself."* (note that a more recent, and precise, definition of computer virus has been given by the Hungarian security researcher Péter Ször: *"a code that recursively replicates a possibly evolved copy of itself"*)

The first IBM PC compatible "in the wild" computer virus, and one of the first real widespread infections, was "Brain" in 1986. From then, the number of viruses has grown exponentially. Most of the computer viruses written in the early and mid-1980s were limited to self-reproduction and had no specific damage routine built into the code. That changed when more and more programmers became acquainted with computer virus programming and created viruses that manipulated or even destroyed data on infected computers.

Before internet connectivity was widespread, computer viruses were typically spread by infected floppy disks. Antivirus software came into use, but was updated relatively infrequently. During this time, virus checkers essentially had to check executable files and the boot sectors of floppy disks and hard disks. However, as internet usage became common, viruses began to spread online.

1980–1990 period (early days)

There are competing claims for the innovator of the first antivirus product. Possibly, the first publicly documented removal of an "in the wild" computer virus (i.e. the "Vienna virus") was performed by Bernd Fix in 1987.

In 1987, Andreas Lüning and Kai Figge founded G Data Software and released their first antivirus product for the Atari ST platform. Dubiously, they later also produced Virus Construction Kits. In 1987, the *Ultimate Virus Killer (UVK)* was also released. This was the de facto industry standard virus killer for the Atari ST and Atari Falcon, the last version of which (version 9.0) was released in April 2004. In 1987, in the United States, John McAfee founded the McAfee company (now part of Intel Security) and, at the end of that year, he released the first version of VirusScan. In the meanwhile, in Slovakia, Peter Paško and Miroslav Trnka created the first version of NOD32antivirus (albeit they established ESET only in 1992).

In 1987, Fred Cohen wrote that **there is no algorithm that can perfectly detect all possible computer viruses.**

Finally, in the end of 1987, the first two heuristic antivirus utilities were released: *FluShot Plus* by Ross Greenberg and *Anti4us* by Erwin Lanting. However, the kind of heuristic they were using was totally different from the one used today by many antivirus products. The first antivirus product with a heuristic engine which resembles the ones used nowadays was F-PROT in 1991. The early heuristic engines were based on dividing the binary in different sections: data section, code section (in legitimate binary it usually starts always from the same location). Indeed, the initial viruses re-organise the layout of the sections, or override the initial portion of section in order to jump to the very end of the file where malicious code was located and then, later on, go back to resume the execution of the original code. This was a very specific pattern, not used at the time by any legitimate software, that initially represented a very nice heuristic to catch where something was suspicious or not. Later, in time, other kind of more advanced heuristics have been added, such as: suspicious sections name, incorrect header size, wildcards and regular expressions and partial pattern in-memory matching.

In 1988, the growth of antivirus companies continued. In Germany, Tjark Auerbach founded Avira (*H+BEDV* at the time) and released the first version of *AntiVir* (named "*Luke Filewalker*" at the time). In Bulgaria, Dr. Vesselin Bontchev released his first freeware antivirus program (he later joined FRISK Software). Also Frans Veldman released the first version of ThunderByte Antivirus, also known as *TBAV* (he sold his company to Norman Safeground in 1998). In Czech Republic, Pavel Baudiš and Eduard Kučera started avast!(at the time *ALWIL Software*) and released their first version of avast! antivirus. In June 1988, in South Korea, Dr. Ahn Cheol-Soo released its first antivirus software, called *V1* (he founded AhnLab later in 1995). Finally, in the Autumn 1988, in United Kingdom, Alan Solomon founded S&S International and created his *Dr. Solomon's Anti-Virus Toolkit*(although he launched it commercially only in 1991 – in 1998 Dr. Solomon's company was

acquired by McAfee). In November 1988 a professor at the Panamerican University in Mexico City named Alejandro E. Carriles copyrighted the first antivirus software in Mexico under the name "Byte Matabichos" (Byte Bugkiller) to help solve the rampant virus infestation among students.

Also in 1988, a mailing list named VIRUS-L was started on the BITNET/EARN network where new viruses and the possibilities of detecting and eliminating viruses were discussed. Some members of this mailing list were: Alan Solomon, Eugene Kaspersky (Kaspersky Lab), Friðrik Skúlason (FRISK Software), John McAfee (McAfee), Luis Corrons (Panda Security), Mikko Hyppönen (F-Secure), Péter Szőr, Tjark Auerbach (Avira) and Dr. Vesselin Bontchev (FRISK Software).

In 1989, in Iceland, Friðrik Skúlason created the first version of F-PROT Anti-Virus back in 1989 (he founded FRISK Software only in 1993). In the meanwhile, in United States, Symantec (founded by Gary Hendrix in 1982) launched its first *Symantec antivirus for Macintosh* (SAM). SAM 2.0, released March 1990, incorporated technology allowing users to easily update SAM to intercept and eliminate new viruses, including many that didn't exist at the time of the program's release.

In the end of the 1980s, in United Kingdom, Jan Hruska and Peter Lammer founded the security firm Sophos and began producing their first antivirus and encryption products. In the same period, in Hungary, also VirusBuster was founded (which has recently being incorporated by Sophos).

1990–2000 period (emergence of the antivirus industry)

In 1990, in Spain, Mikel Urizarbarrena founded Panda Security (*Panda Software* at the time). In Hungary, the security researcher Péter Szőr released the first version of *Pasteur* antivirus. In Italy, Gianfranco Tonello created the first version of VirIT eXplorer antivirus (he founded TG Soft one year later).

In 1990, the Computer Antivirus Research Organization (CARO) was founded. In 1991, CARO released the "*Virus Naming Scheme*", originally written by Friðrik Skúlason and Vesselin Bontchev. Although this naming scheme is now outdated, it remains the only existing standard that most computer security companies and researchers ever attempted to adopt. CARO members includes: Alan Solomon, Costin Raiu, Dmitry Gryaznov, Eugene Kaspersky, Friðrik Skúlason, Igor Muttik, Mikko Hyppönen, Morton Swimmer, Nick Fitzgerald, Padgett Peterson, Peter Ferrie, Righard Zwienenberg and Dr. Vesselin Bontchev.

In 1991, in the United States, Symantec released the first version of Norton Anti-Virus. In the same year, in Czechoslovakia, Jan Gritzbaach and Tomáš Hofer founded AVG Technologies (*Grisoft* at the time), although they released the first version of their *Anti-Virus Guard* (AVG) only in 1992. On the other hand, in Finland, F-Secure (founded in 1988 by Petri Allas and Risto Siilasmaa – with the name

of Data Fellows) released the first version of their antivirus product. F-Secure claims to be the first antivirus firm to establish a presence on the World Wide Web.

In 1991, the European Institute for Computer Antivirus Research (EICAR) was founded to further antivirus research and improve development of antivirus software.

In 1992, in Russia, Igor Danilov released the first version of *SpiderWeb*, which later became Dr. Web.

In 1994, AV-TEST reported that there were 28,613 unique malware samples (based on MD5) in their database.

Over time other companies were founded. In 1996, in Romania, Bitdefender was founded and released the first version of *Anti-Virus eXpert* (AVX). In 1997, in Russia, Eugene Kaspersky and Natalia Kaspersky co-founded security firm Kaspersky Lab.

In 1996, there was also the first "in the wild" Linux virus, known as "*Staog*".

In 1999, AV-TEST reported that there were 98,428 unique malware samples (based on MD5) in their database.

2000–2005 period

In 2000, Rainer Link and Howard Fuhs started the first open source antivirus engine, called *OpenAntivirus Project*.

In 2001, Tomasz Kojm released the first version of ClamAV, the first ever open source antivirus engine to be commercialised. In 2007, ClamAV was bought by Sourcefire, which in turn was acquired by Cisco Systems in 2013.

In 2002, in United Kingdom, Morten Lund and Theis Søndergaard co-founded the antivirus firm BullGuard.

In 2005, AV-TEST reported that there were 333,425 unique malware samples (based on MD5) in their database.

2005 to present

In 2007, AV-TEST reported a number of 5,490,960 new unique malware samples (based on MD5) only for that year. In 2012 and 2013, antivirus firms reported a new malware samples range from 300,000 to over 500,000 per day.

Over the years it has become necessary for antivirus software to use several different strategies (e.g. specific email and network protection or low level modules) and detection algorithms, as well as to check an increasing variety of files, rather than just executables, for several reasons:

- Powerful macros used in word processor applications, such as Microsoft Word, presented a risk. Virus writers could use the macros to write viruses embedded within documents. This meant that computers could now also be at risk from infection by opening documents with hidden attached macros.
- The possibility of embedding executable objects inside otherwise non-executable file formats can make opening those files a risk.
- Later email programs, in particular Microsoft's Outlook Express and Outlook, were vulnerable to viruses embedded in the email body itself. A user's computer could be infected by just opening or previewing a message.

In 2005, F-Secure was the first security firm that developed an Anti-Rootkit technology, called *BlackLight*.

Given the consideration that most of the people is nowadays connected to the Internet round-the-clock, in 2008, Jon Oberheide first proposed a Cloud-based antivirus design.

In February 2008 McAfee Labs added the industry-first cloud-based anti-malware functionality to VirusScan under Artemis name. It was tested by AV-Comparatives in February 2008 and officially unveiled in August 2008 in McAfee VirusScan.

Cloud AV created problems for comparative testing of security software – part of the AV definitions was out of testers control (on constantly updated AV company servers) thus making results non-repeatable. As a result, Anti-Malware Testing Standards Organisation (AMTSO) started working on methodology of testing cloud products which was adopted on 7 May 2009.

In 2011, AVG introduced a similar cloud service, called Protective Cloud Technology.

Most recently, the industry has seen approaches to the problem of detecting and mitigating Zero-day attacks. One method from Bromium involves micro-virtualization to protect desktops from malicious code execution initiated by the end user. Another approach from SentinelOne focuses on behavioral detection by building a full context around every process execution path in real time.

Identification methods

One of the few solid theoretical results in the study of computer viruses is Frederick B. Cohen's 1987 demonstration that there is no algorithm that can perfectly detect all possible viruses. However, using different layers of defense, a good detection rate may be achieved.

There are several methods which antivirus engine can use to identify malware:

- **Sandbox detection:** is a particular behavioural-based detection technique that, instead of detecting the behavioural fingerprint at run time, it executes the programs in a virtual environment, logging what actions the program performs. Depending on the actions logged, the antivirus engine can determine if the program is malicious or not. If not, then, the program is executed in the real environment. Albeit this technique has shown to be quite effective, given its heaviness and slowness, it is rarely used in end-user antivirus solutions.
- **Data mining techniques:** are one of the latest approach applied in malware detection. Data mining and machine learning algorithms are used to try to classify the behaviour of a file (as either malicious or benign) given a series of file features, that are extracted from the file itself.

Signature-based detection

Traditional antivirus software relies heavily upon signatures to identify malware.

Substantially, when a malware arrives in the hands of an antivirus firm, it is analysed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software.

Although the signature-based approach can effectively contain malware outbreaks, malware authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and, more recently, "metamorphic" viruses, which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary.

Heuristics

Many viruses start as a single infection and through either mutation or refinements by other attackers, can grow into dozens of slightly different strains, called variants. Generic detection refers to the detection and removal of multiple threats using a single virus definition.

For example, the Vundo trojan has several family members, depending on the antivirus vendor's classification. Symantec classifies members of the Vundo family into two distinct categories, *Trojan.Vundo* and *Trojan.Vundo.B*.

While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a generic signature or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie. These wildcards allow the scanner to detect viruses even if they are padded with extra, meaningless code. A detection that uses this method is said to be "heuristic detection."

Rootkit detection

Anti-virus software can attempt to scan for rootkits. A rootkit is a type of malware designed to gain administrative-level control over a computer system without being detected. Rootkits can change how the operating system functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult to remove, in some cases requiring a complete re-installation of the operating system.

Real-time protection

Real-time protection, on-access scanning, background guard, resident shield, autoprotect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs. This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects in 'real-time', in other words while data loaded into the computer's active memory: when inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed.

Issues of concern

Unexpected renewal costs

Some commercial antivirus software end-user license agreements include a clause that the subscription will be automatically renewed, and the purchaser's credit card automatically billed, at the renewal time without explicit approval. For example, McAfee requires users to unsubscribe at least 60 days before the expiration of the present subscription while BitDefender sends notifications to unsubscribe 30 days before the renewal. Norton AntiVirus also renews subscriptions automatically by default.

Rogue security applications

Some apparent antivirus programs are actually malware masquerading as legitimate software, such as WinFixer, MS Antivirus, and Mac Defender.

Problems caused by false positives

A "false positive" or "false alarm" is when antivirus software identifies a non-malicious file as malware. When this happens, it can cause serious problems. For example, if an antivirus program is configured to immediately delete or quarantine infected files, as is common on Microsoft Windows antivirus applications, a false positive in an essential file can render the Windows operating system or some applications unusable. Recovering from such damage to critical software infrastructure incurs technical support costs and businesses can be forced to close whilst remedial action is undertaken. For example, in May 2007 a faulty virus signature issued by Symantec mistakenly removed essential operating system files, leaving thousands of PCs unable to boot.

Also in May 2007, the executable file required by Pegasus Mail on Windows was falsely detected by Norton AntiVirus as being a Trojan and it was automatically removed, preventing Pegasus Mail from running. Norton AntiVirus had falsely identified three releases of Pegasus Mail as malware, and would delete the Pegasus Mail installer file when that happened.^[112] In response to this Pegasus Mail stated:

“ On the basis that Norton/Symantec has done this for every one of the last three releases of Pegasus Mail, we can only condemn this product as too flawed to use, and recommend in the strongest terms that our users cease using it in favour of alternative, less buggy anti-virus packages. ”

In April 2010, McAfee VirusScan detected svchost.exe, a normal Windows binary, as a virus on machines running Windows XP with Service Pack 3, causing a reboot loop and loss of all network access.

In December 2010, a faulty update on the AVG anti-virus suite damaged 64-bit versions of Windows 7, rendering it unable to boot, due to an endless boot loop created.

In October 2011, Microsoft Security Essentials (MSE) removed the Google Chrome web browser, rival to Microsoft's own Internet Explorer. MSE flagged Chrome as a Zbot banking trojan.

In September 2012, Sophos' anti-virus suite identified various update-mechanisms, including its own, as malware. If it was configured to automatically delete detected files, Sophos Antivirus could render itself unable to update, required manual intervention to fix the problem.

System and interoperability related issues

Running (the real-time protection of) multiple antivirus programs concurrently can degrade performance and create conflicts. However, using a concept called multiscanning, several companies (including G Data and Microsoft) have created applications which can run multiple engines concurrently.

It is sometimes necessary to temporarily disable virus protection when installing major updates such as Windows Service Packs or updating graphics card drivers. Active antivirus protection may partially or completely prevent the installation of a major update. Anti-virus software can cause problems during the installation of an operating system upgrade, e.g. when upgrading to a newer version of Windows "in place" — without erasing the previous version of Windows. Microsoft recommends that anti-virus software be disabled to avoid conflicts with the upgrade installation process.

The functionality of a few computer programs can be hampered by active anti-virus software. For example, TrueCrypt, a disk encryption program, states on its troubleshooting page that anti-virus programs can conflict with TrueCrypt and cause it to malfunction or operate very slowly. Anti-virus software can impair the performance and stability of games running in the Steam platform.

Support issues also exist around antivirus application interoperability with common solutions like SSL VPN remote access and network access control products. These technology solutions often have policy assessment applications which require that an up-to-date antivirus is installed and running. If the antivirus application is not recognized by the policy assessment, whether because the antivirus application has been updated or because it is not part of the policy assessment library, the user will be unable to connect.

Effectiveness

Studies in December 2007 showed that the effectiveness of antivirus software had decreased in the previous year, particularly against unknown or [zero day attacks](#). The computer magazine *c't* found that detection rates for these threats had dropped from 40–50% in 2006 to 20–30% in 2007. At that time, the only exception was the [NOD32](#) antivirus, which managed a detection rate of 68%. According to the *Zeus tracker* website the average detection rate for all variants of the well-known [Zeus](#) trojan is as low as 40%.

The problem is magnified by the changing intent of virus authors. Some years ago it was obvious when a virus infection was present. The viruses of the day, written by amateurs, exhibited destructive behavior or pop-ups. Modern viruses are often written by professionals, financed by criminal organizations.

In 2008, Eva Chen, CEO of Trend Micro, stated that the anti-virus industry has over-hyped how effective its products are — and so has been misleading customers — for years.

Independent testing on all the major virus scanners consistently shows that none provide 100% virus detection. The best ones provided as high as 99.9% detection for simulated real-world situations, while the lowest provided 91.1% in tests conducted in August 2013. Many virus scanners produce false positive results as well, identifying benign files as malware.

Although methodologies may differ, some notable independent quality testing agencies include AV-Comparatives, ICSA Labs, West Coast Labs, Virus Bulletin, AV-TEST and other members of the Anti-Malware Testing Standards Organization.

New viruses

Anti-virus programs are not always effective against new viruses, even those that use non-signature-based methods that should detect new viruses. The reason for this is that the virus designers test their new viruses on the major anti-virus applications to make sure that they are not detected before releasing them into the wild.

Some new viruses, particularly ransomware, use polymorphic code to avoid detection by virus scanners. Jerome Segura, a security analyst with ParetoLogic, explained:

“ *It's something that they miss a lot of the time because this type of [ransomware virus] comes from sites that use a polymorphism, which means they basically randomize the file they send you and it gets by well-known antivirus products very easily. I've seen people firsthand getting infected, having all the pop-ups and yet they have antivirus software running and it's not detecting anything. It actually can be pretty hard to get rid of, as well, and you're never really sure if it's really gone. When we see something like that usually we advise to reinstall the operating system or reinstall backups.*

”

A proof of concept virus has used the Graphics Processing Unit (GPU) to avoid detection from anti-virus software. The potential success of this involves bypassing the CPU in order to make it much harder for security researchers to analyse the inner workings of such malware.

Rootkits

Detecting rootkits is a major challenge for anti-virus programs. Rootkits have full administrative access to the computer and are invisible to users and hidden from the list of running processes in the task manager. Rootkits can modify the inner workings of the operating system and tamper with antivirus programs.

Damaged files

If a file has been infected by a computer virus, anti-virus software will attempt to remove the virus code from the file during disinfection, but it is not always able to restore the file to its undamaged state. In such circumstances, damaged files can only be restored from existing backups or shadow copies (this is also true for ransomware); installed software that is damaged requires re-installation.

Firmware issues

Active anti-virus software can interfere with a firmware update process. Any writeable firmware in the computer can be infected by malicious code. This is a major concern, as an infected BIOS could require the actual BIOS chip to be replaced to ensure the malicious code is completely removed. Anti-virus software is not effective at protecting firmware and the motherboard BIOS from infection. In 2014, security researchers discovered that USB devices contain writeable firmware which can be modified with malicious code (dubbed "BadUSB"), which anti-virus software cannot detect or prevent. The malicious code can run undetected on the computer and could even infect the operating system prior to it booting up.

Performance and other drawbacks

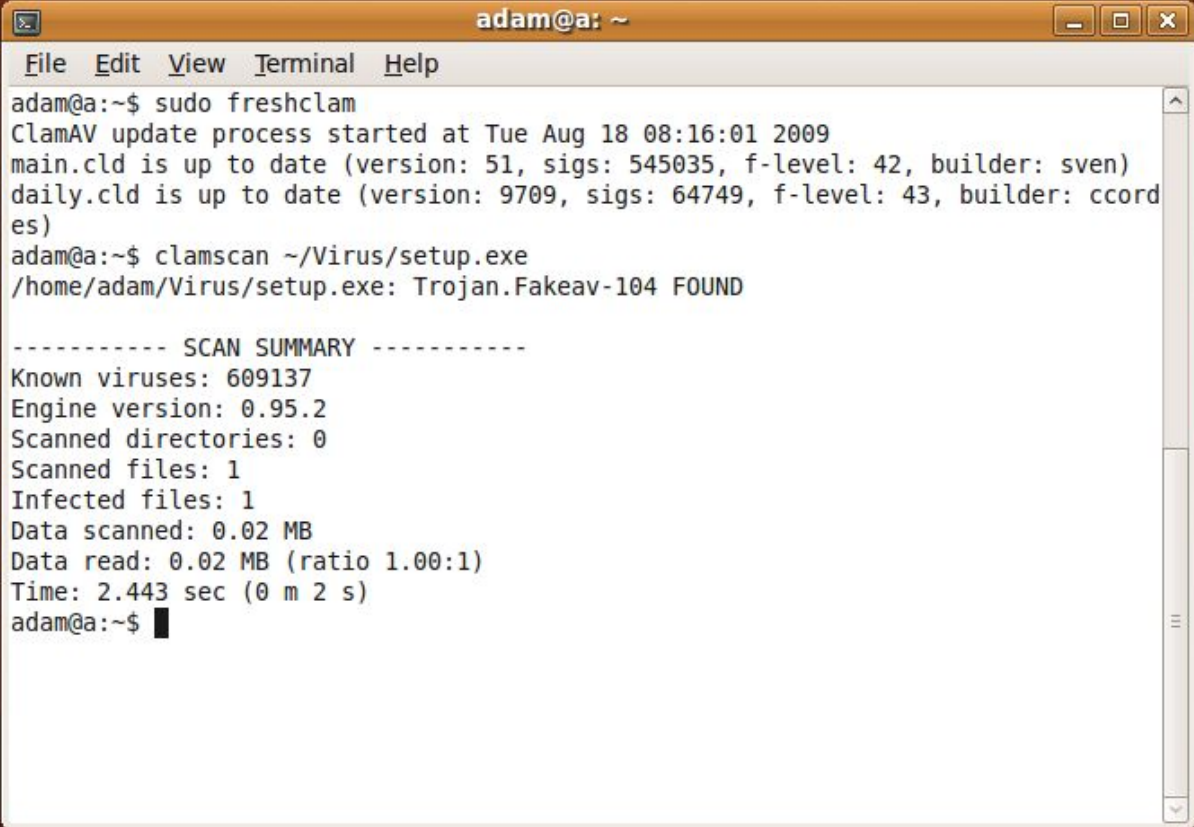
Antivirus software has some drawbacks, first of which that it can impact a computer's performance.

Furthermore, inexperienced users can be lulled into a false sense of security when using the computer, considering themselves to be invulnerable, and may have problems understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach. If the antivirus software employs heuristic detection, it must be fine-tuned to minimize misidentifying harmless software as malicious (false positive).

Antivirus software itself usually runs at the highly trusted kernel level of the operating system to allow it access to all the potential malicious process and files, creating a potential avenue of attack. The UK and US intelligence agencies, GCHQ and the National Security Agency (NSA), respectively, have been exploiting anti-virus software to spy on users. Anti-virus software has highly privileged and trusted access to the underlying operating system, which makes it a much more appealing target for remote attacks. Additionally anti-virus software is "years behind security-conscious client-side applications like browsers or document readers", according to Joxean Koret, a researcher with Coseinc, a Singapore-based information security consultancy.

Alternative solutions

Installed antivirus solutions, running on individual computers, although the most used, is only one method of guarding against malware. Other alternative solutions are also used, including: Unified Threat Management (UTM), hardware and network firewalls, Cloud-based antivirus and on-line scanners.

A screenshot of a terminal window titled 'adam@a: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', and 'Help'. The terminal output shows the execution of 'sudo freshclam' which updates ClamAV signatures, followed by 'clamscan ~/Virus/setup.exe' which identifies a Trojan. A detailed scan summary follows, showing 609137 known viruses, 0.95.2 engine version, and 1 infected file. The window includes standard OS window controls (minimize, maximize, close) and a vertical scrollbar on the right.

```
adam@a:~$ sudo freshclam
ClamAV update process started at Tue Aug 18 08:16:01 2009
main.cld is up to date (version: 51, sigs: 545035, f-level: 42, builder: sven)
daily.cld is up to date (version: 9709, sigs: 64749, f-level: 43, builder: ccorde
es)
adam@a:~$ clamscan ~/Virus/setup.exe
/home/adam/Virus/setup.exe: Trojan.Fakeav-104 FOUND

----- SCAN SUMMARY -----
Known viruses: 609137
Engine version: 0.95.2
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.02 MB
Data read: 0.02 MB (ratio 1.00:1)
Time: 2.443 sec (0 m 2 s)
adam@a:~$
```

The command-line virus scanner of Clam AV 0.95.2, an open source antivirus originally developed by Tomasz Kojm in 2001. Here running a virus signature definition update, scanning a file and identifying a Trojan.

Hardware and network firewall

Network firewalls prevent unknown programs and processes from accessing the system. However, they are not antivirus systems and make no attempt to identify or remove anything. They may protect against infection from outside the protected computer or network, and limit the activity of any malicious software which is present by blocking incoming or outgoing requests on certain TCP/IP ports. A firewall is designed to deal with broader system threats that come from network connections into the system and is not an alternative to a virus protection system.

Cloud antivirus

Cloud antivirus is a technology that uses lightweight agent software on the protected computer, while offloading the majority of data analysis to the provider's infrastructure.

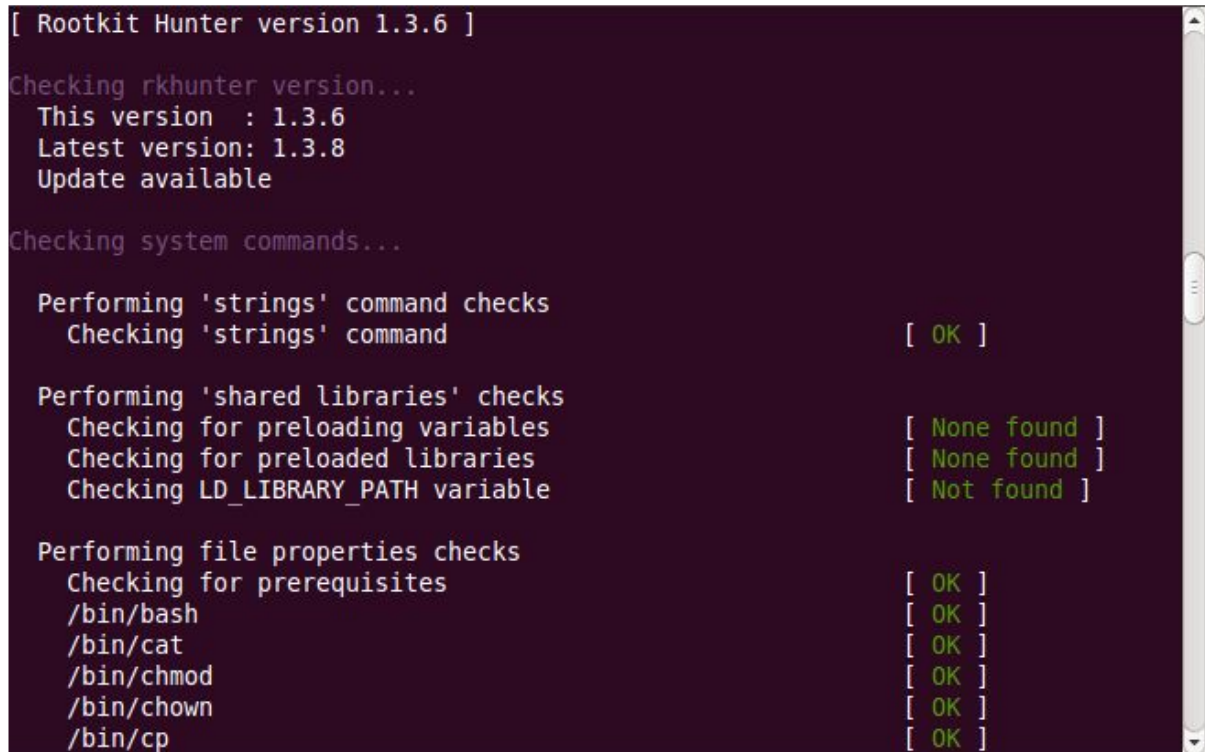
One approach to implementing cloud antivirus involves scanning suspicious files using multiple antivirus engines. This approach was proposed by an early implementation of the cloud antivirus concept called CloudAV. CloudAV was designed to send programs or documents to a network cloud where multiple antivirus and behavioral detection programs are used simultaneously in order to improve detection rates. Parallel scanning of files using potentially incompatible antivirus scanners is achieved by spawning a virtual machine per detection engine and therefore eliminating any possible issues. CloudAV can also perform "retrospective detection," whereby the cloud detection engine rescans all files in its file access history when a new threat is identified thus improving new threat detection speed. Finally, CloudAV is a solution for effective virus scanning on devices that lack the computing power to perform the scans themselves.

Some examples of cloud anti-virus products are Panda Cloud Antivirus, CrowdStrike, Cb Defense and Immunit. Comodo group has also produced cloud-based anti-virus.

Online scanning

Some antivirus vendors maintain websites with free online scanning capability of the entire computer, critical areas only, local disks, folders or files. Periodic online scanning is a good idea for those that run antivirus applications on their computers because those applications are frequently slow to catch threats. One of the first things that malicious software does in an attack is disable any existing antivirus software and sometimes the only way to know of an attack is by turning to an online resource that is not installed on the infected computer.

Specialist tools



```
[ Rootkit Hunter version 1.3.6 ]

Checking rkhunter version...
  This version   : 1.3.6
  Latest version: 1.3.8
  Update available

Checking system commands...

Performing 'strings' command checks
  Checking 'strings' command                [ OK ]

Performing 'shared libraries' checks
  Checking for preloading variables          [ None found ]
  Checking for preloaded libraries          [ None found ]
  Checking LD_LIBRARY_PATH variable         [ Not found ]

Performing file properties checks
  Checking for prerequisites                [ OK ]
  /bin/bash                                [ OK ]
  /bin/cat                                  [ OK ]
  /bin/chmod                                [ OK ]
  /bin/chown                                [ OK ]
  /bin/cp                                   [ OK ]
```

The command-line rkhunter scanner, an engine to scan for Linux rootkits. Here running the tool on Ubuntu.

Virus removal tools are available to help remove stubborn infections or certain types of infection. Examples include Trend Micro's *Rootkit Buster*, and rkhunter for the detection of rootkits, Avira's *AntiVir Removal Tool*, *PCTools Threat Removal Tool*, and AVG's Anti-Virus Free 2011.

A rescue disk that is bootable, such as a CD or USB storage device, can be used to run antivirus software outside of the installed operating system, in order to remove infections while they are dormant. A bootable antivirus disk can be useful when, for example, the installed operating system is no longer bootable or has malware that is resisting all attempts to be removed by the installed antivirus software. Examples of some of these bootable disks include the *Avira AntiVir Rescue System*, *PCTools Alternate Operating System Scanner*, and *AVG Rescue CD*. The AVG Rescue CD software can also be installed onto a USB storage device, that is bootable on newer computers.

Usage and risks

According to an FBI survey, major businesses lose \$12 million annually dealing with virus incidents. A survey by Symantec in 2009 found that a third of small to medium-sized business did not use antivirus protection at that time, whereas more than 80% of home users had some kind of antivirus installed. According to a sociological survey conducted by G Data Software in 2010 49% of women did not use any antivirus program at all.